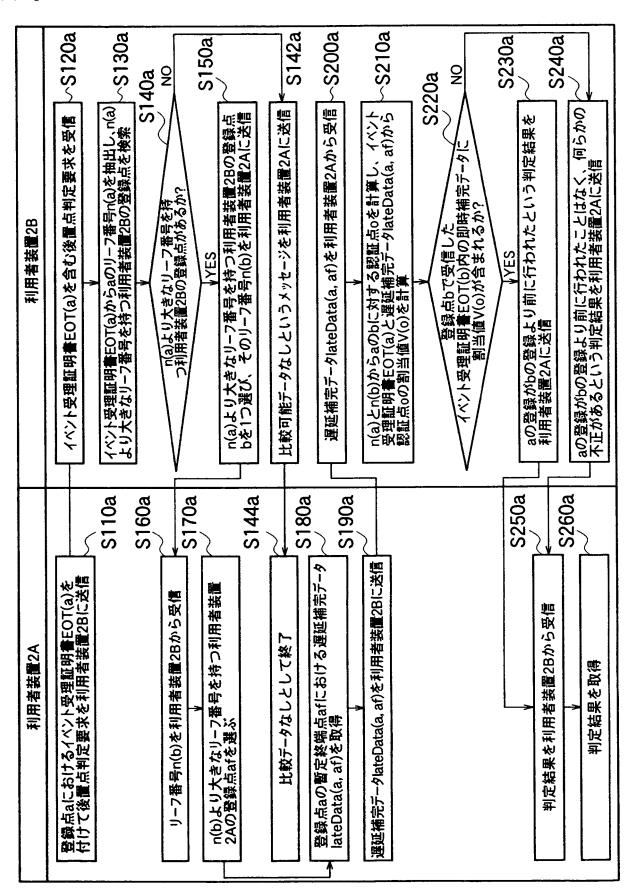
This page is not part of the document!

JP2005015085 / 2006-019143 3/3

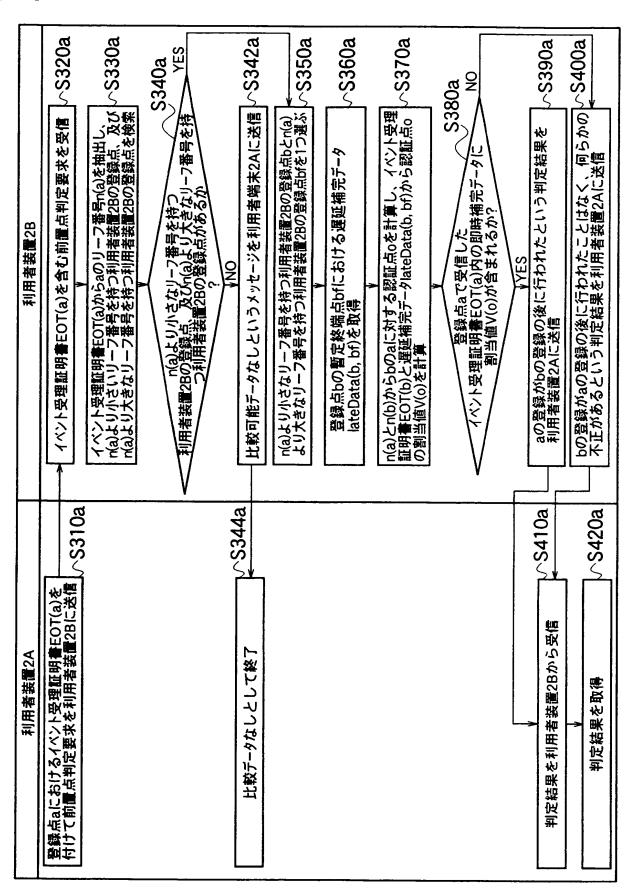
Date: Feb 23, 2006

Recipient: IB

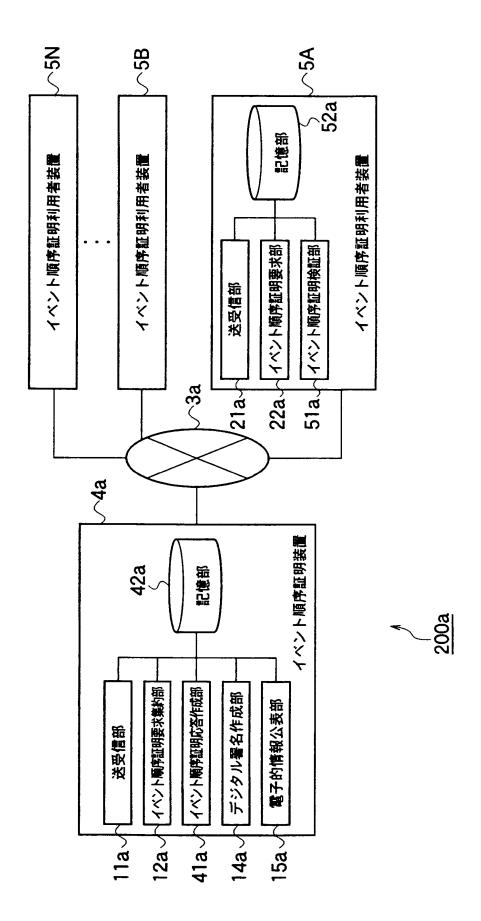
[図40]



[図41]



[図42]

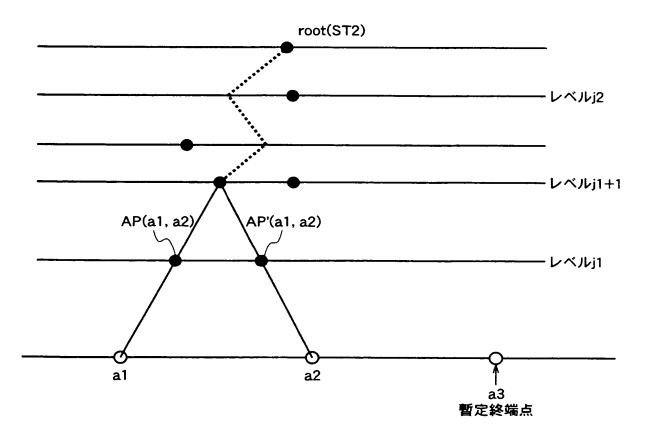


WO 2006/019143 PCT/JP2005/015085 39/77

[図43]

項目	記号	必須	
元デジタルデータ	У	0	
順次割当データ	z	0	
順次集約木識別番号	n	0	Aベント順序受理証明書 EOC(y)
順次集約木リーフ番号	i	0	2000)
登録点の即時補完データ(位置情報、割当値)	sĸ	0	
直前登録点の遅延補完データ(位置情報、割当値)	TK2	0	

[図44]

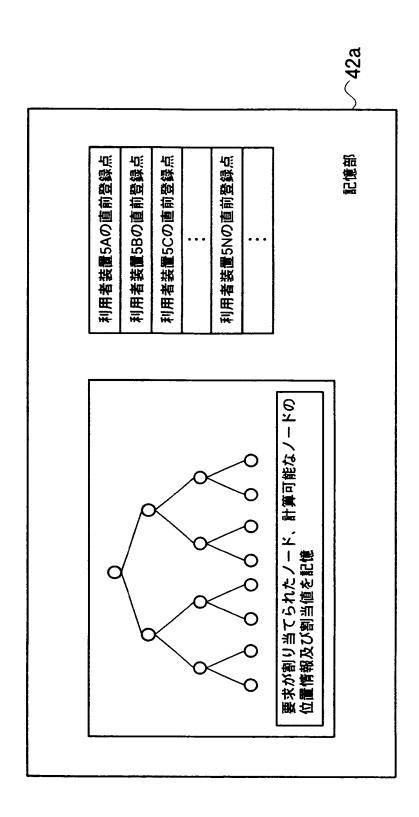


[図45]

登録点	al	a2	a3	a4	a5
即時補完データ	aĵ	a2 ~ P2	a3P6	a4	a5
遅延補完データ		al∿P3	a2~P1	a ³ ~P5\	a4 1
			-a-	a2cp7	- - -
			P4	7 8	
				<i>,</i>	<u></u>

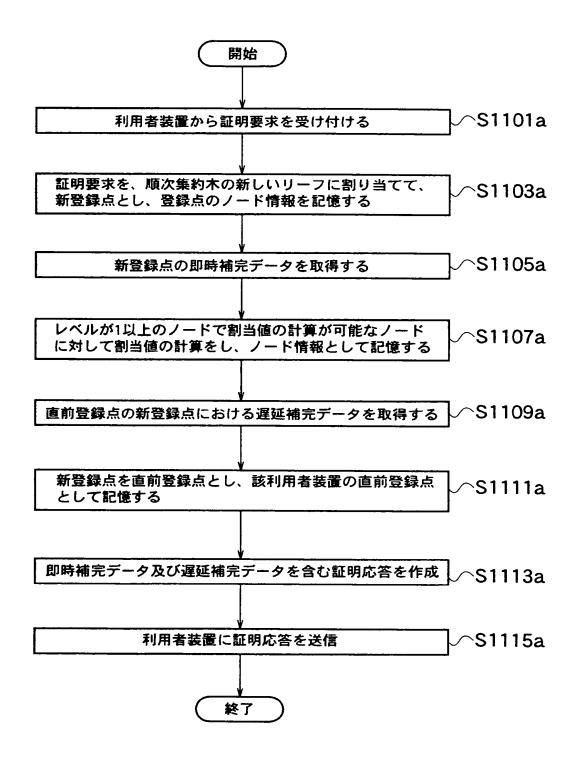
WO 2006/019143 PCT/JP2005/015085 41/77

[図46]

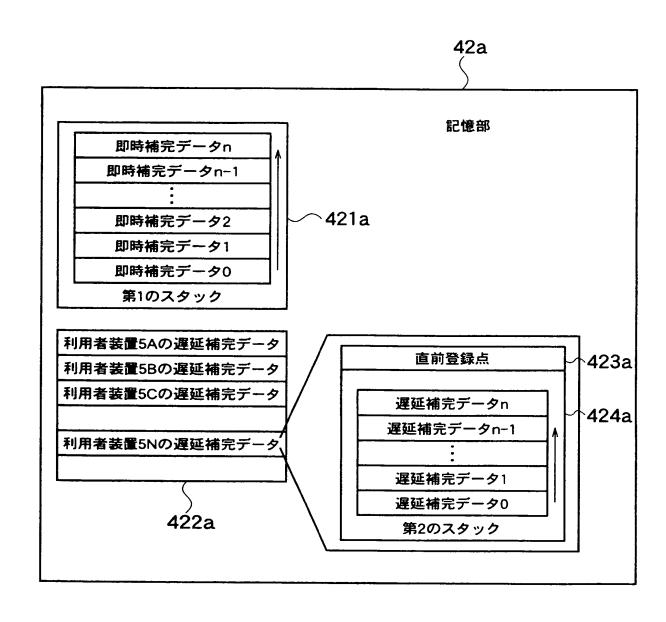


42/77

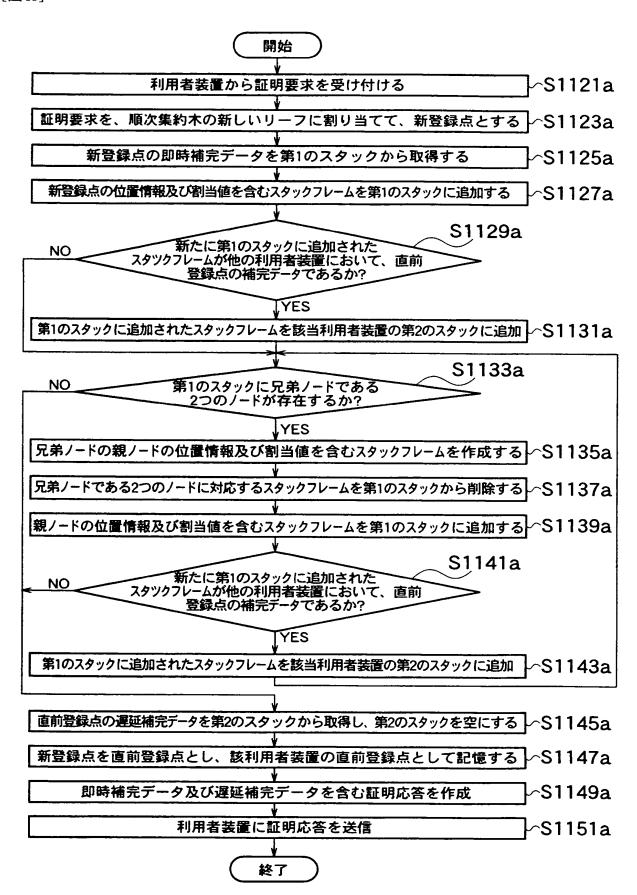
[図47]



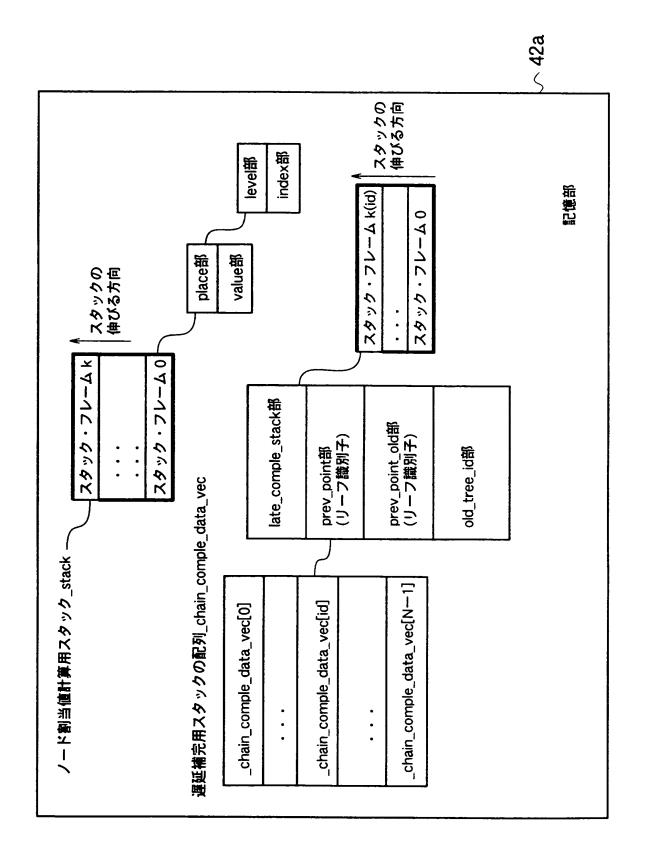
[図48]



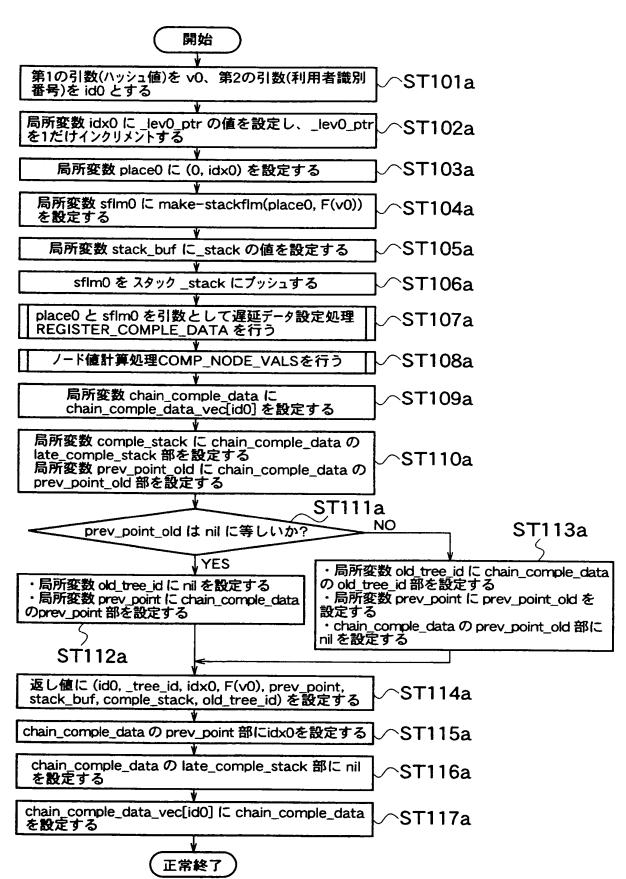
[図49]



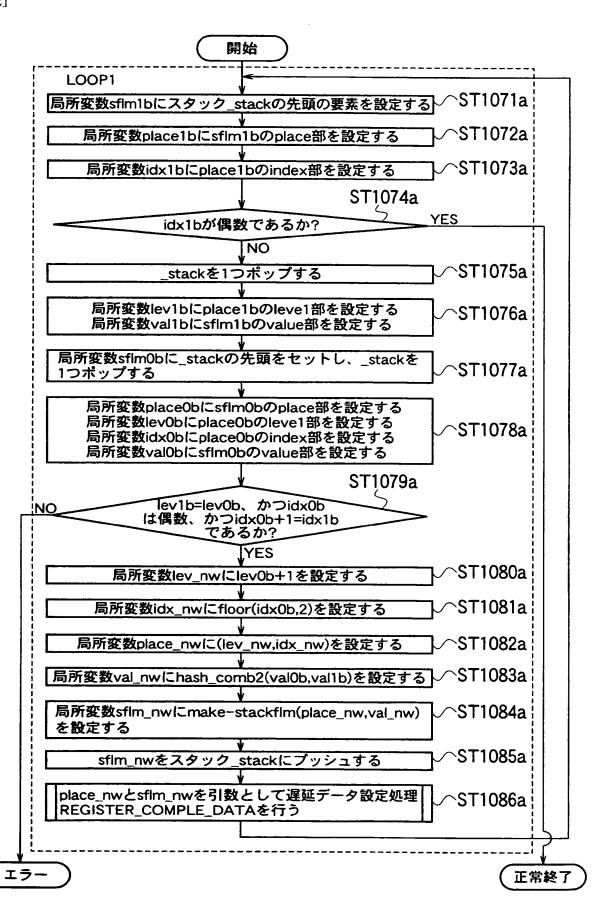
[図50]



[図51]



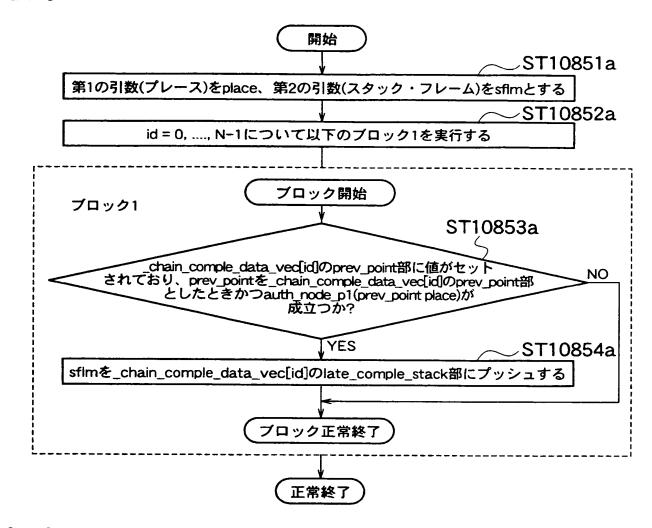
[図52]



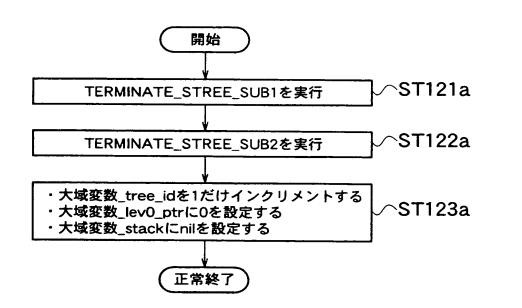
WO 2006/019143 PCT/JP2005/015085

48/77

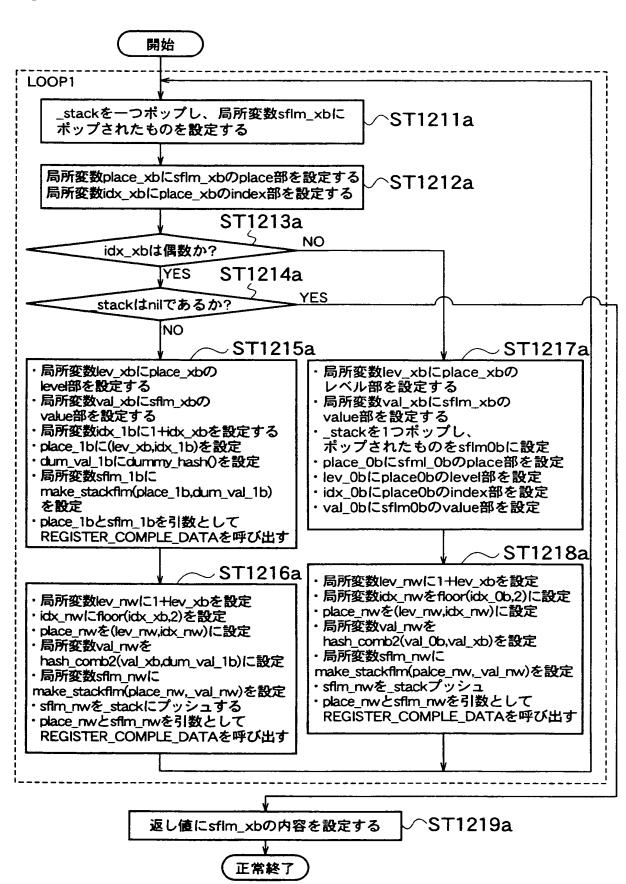
[図53]



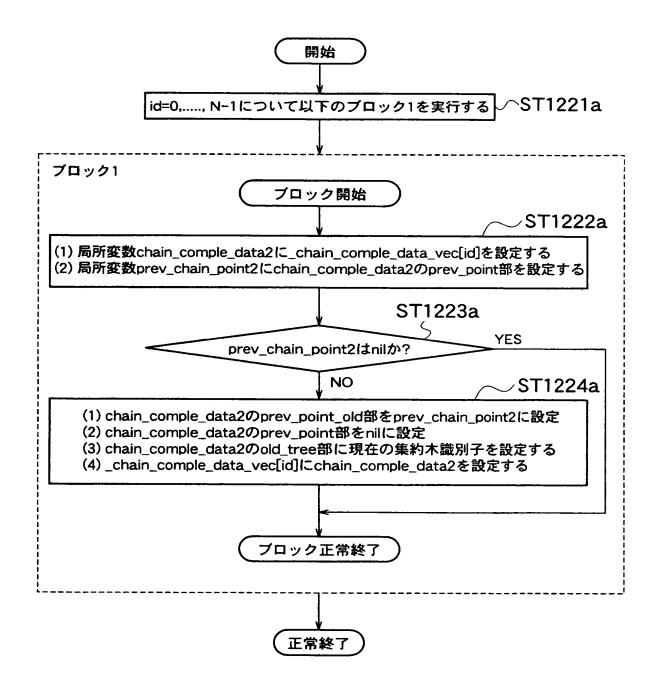
[図54]



[図55]

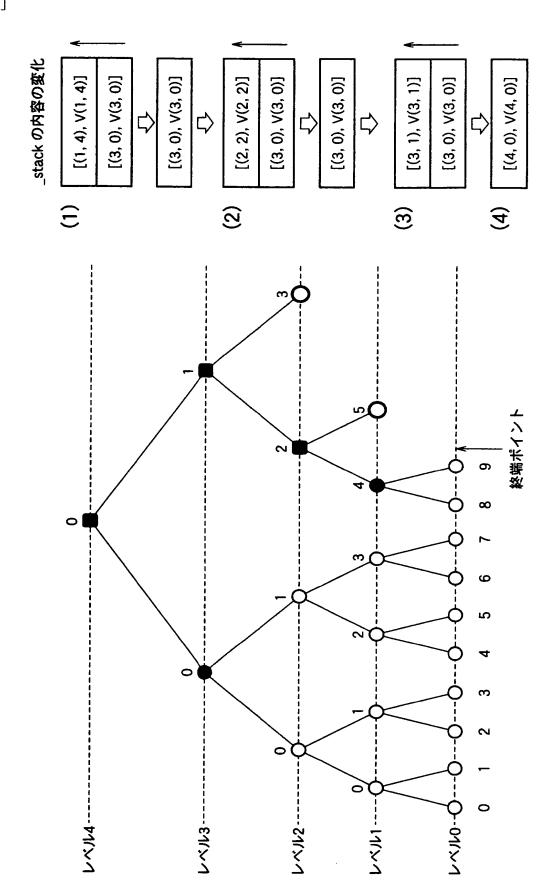


[図56]

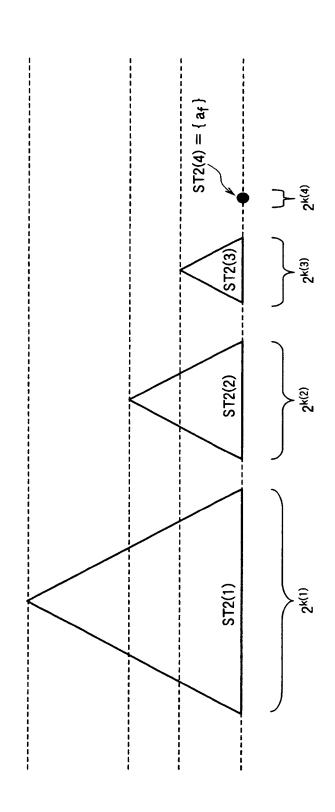


WO 2006/019143 PCT/JP2005/015085 51/77

[図57]

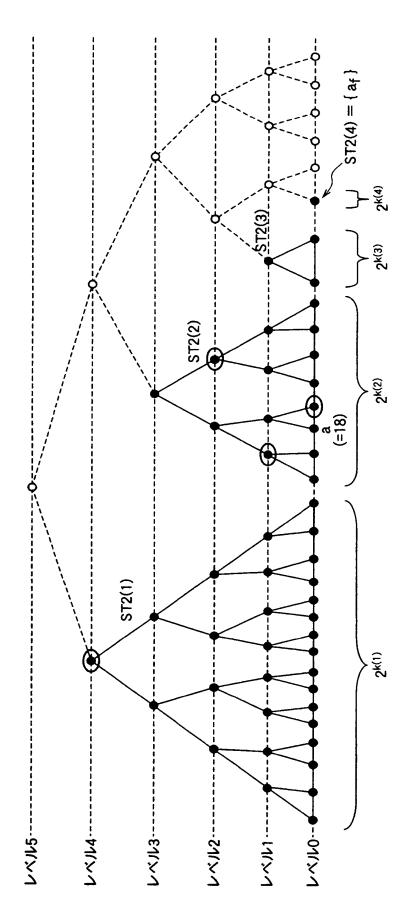


[図58]



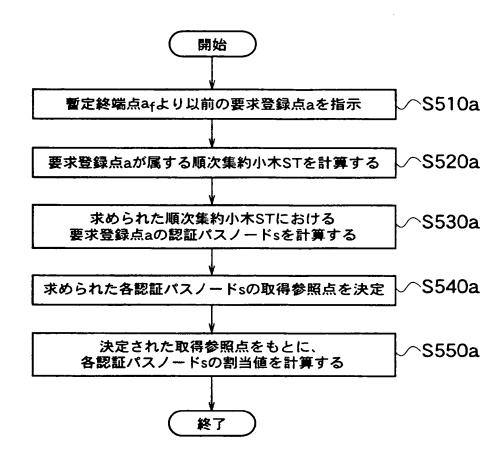
x(1) > k(2) > k(3) > k(4) = 0

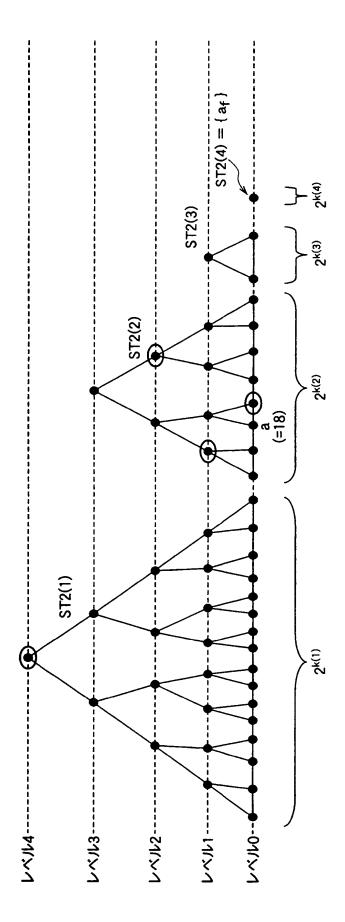
[図59]



k(1)=4 > k(2)=3 > k(3)=1 > k(4)=0

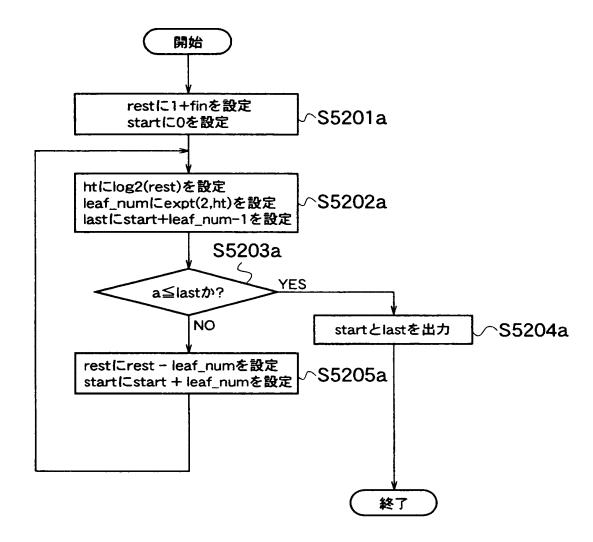
[図60]



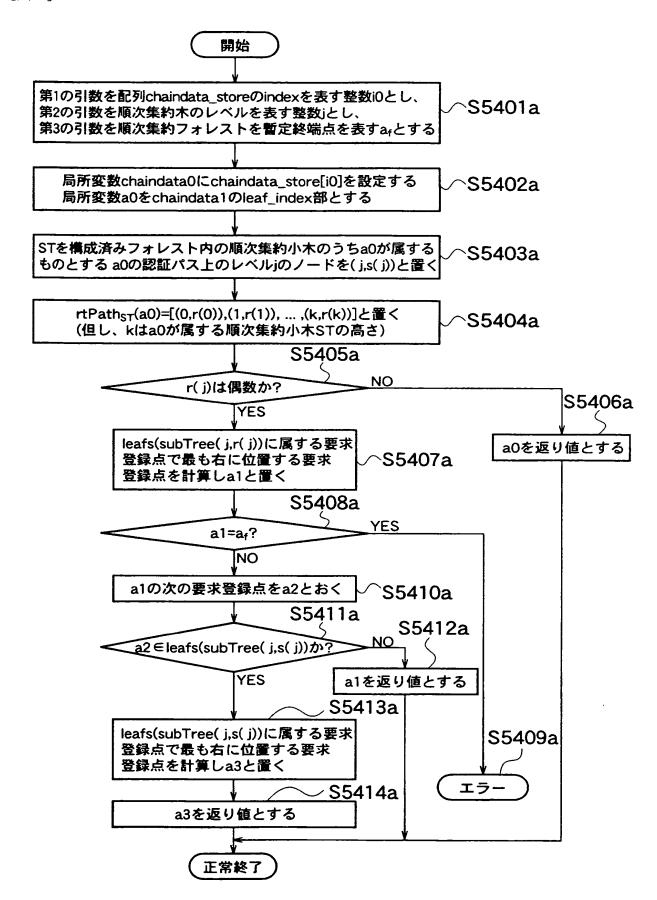


k(1)=4 > k(2)=3 > k(3)=1 > k(4)=0

[図62]



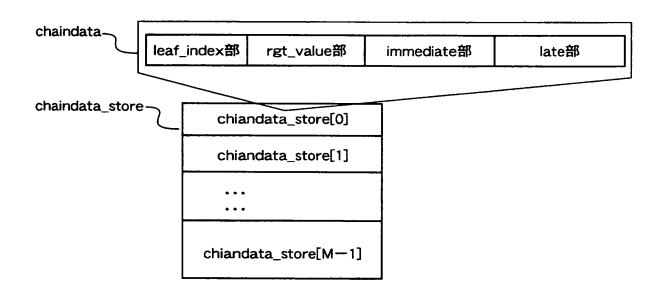
[図63]



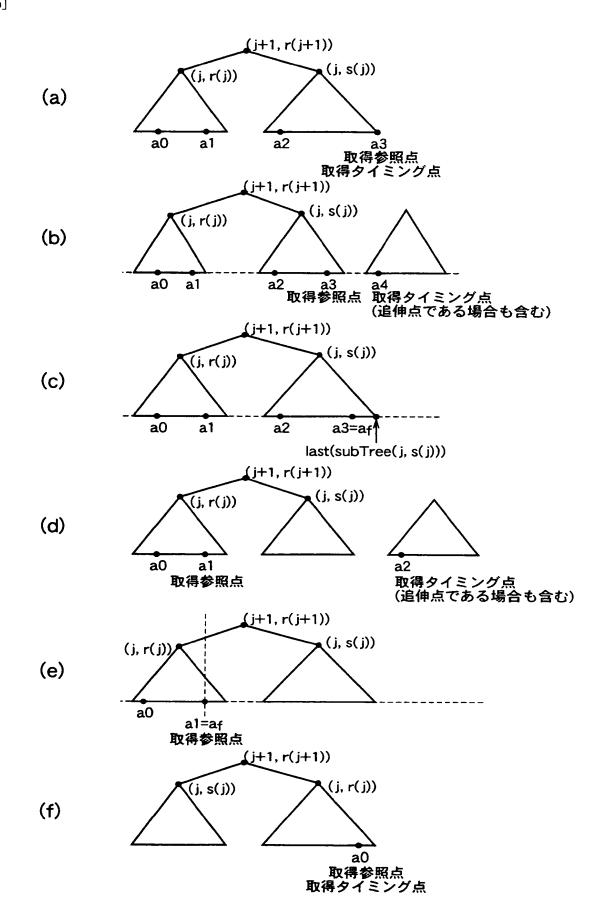
WO 2006/019143 PCT/JP2005/015085

58/77

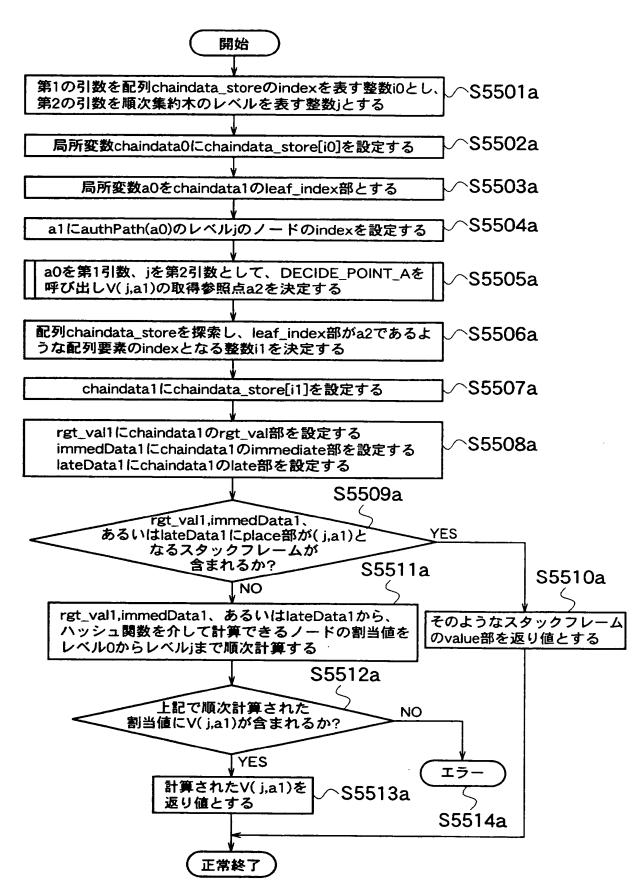
[図64]



[図65]

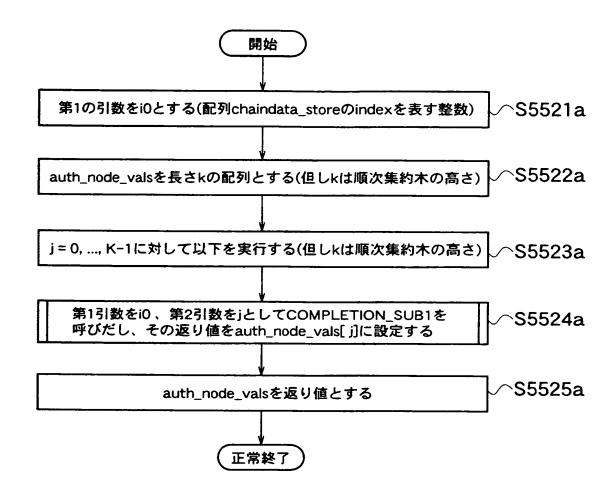


[図66]

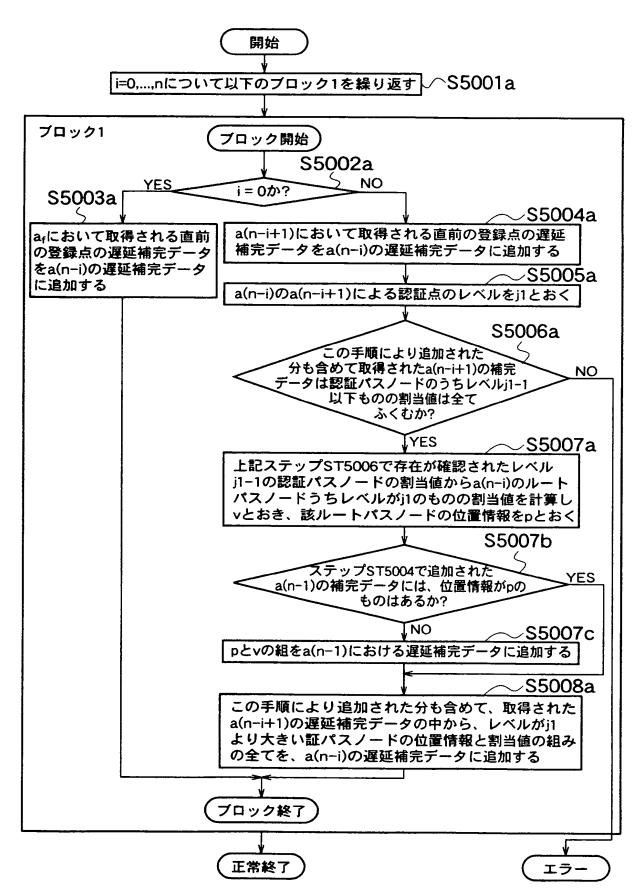


WO 2006/019143 PCT/JP2005/015085 61/77

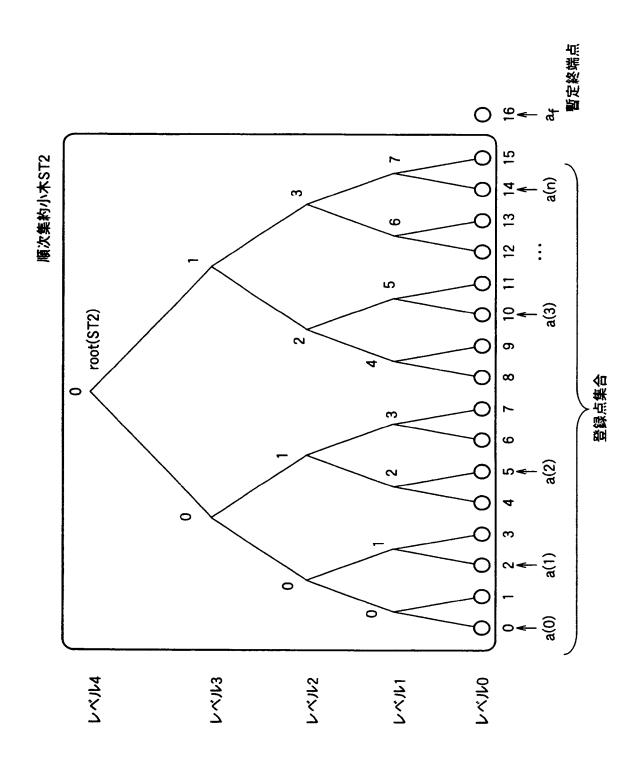
[図67]

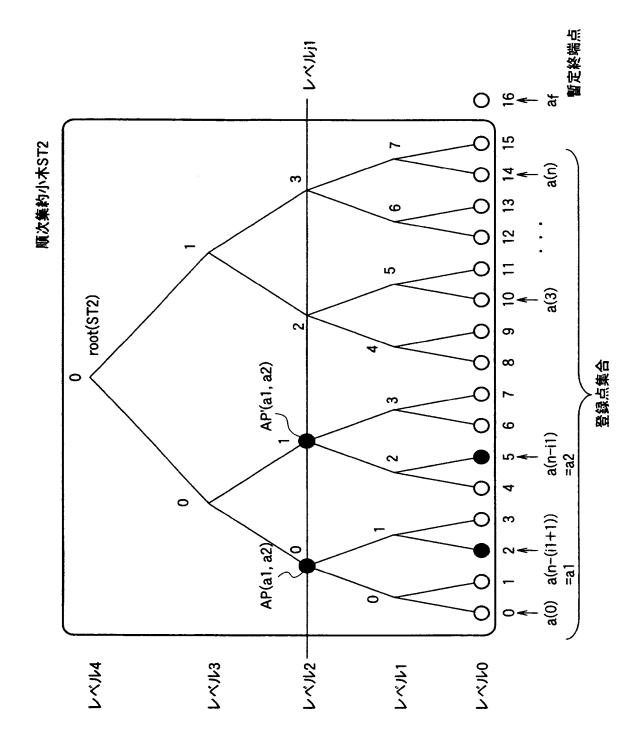


[図68]

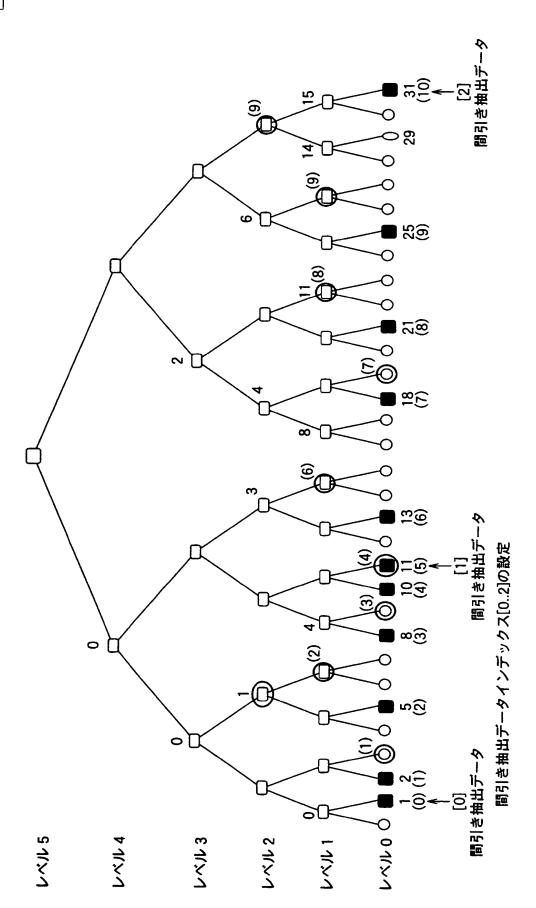


[図69]

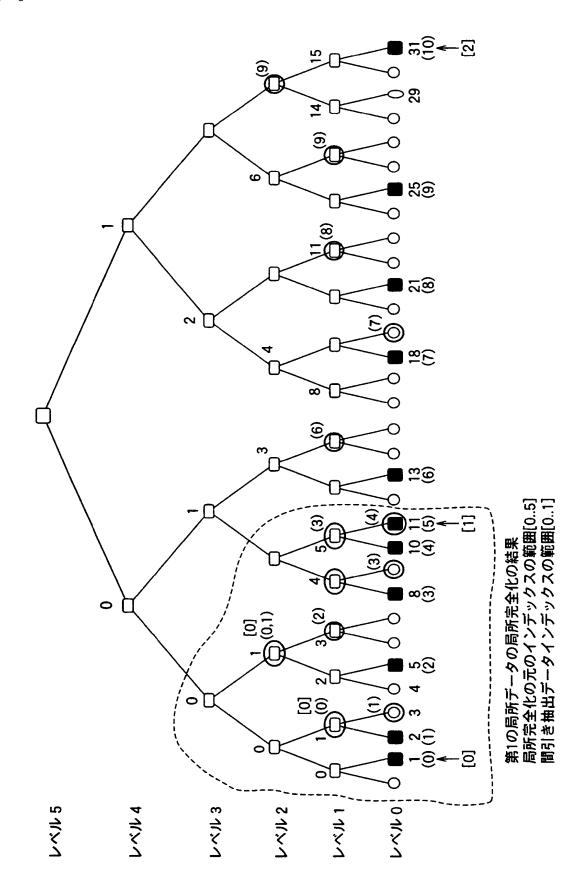




[図71]

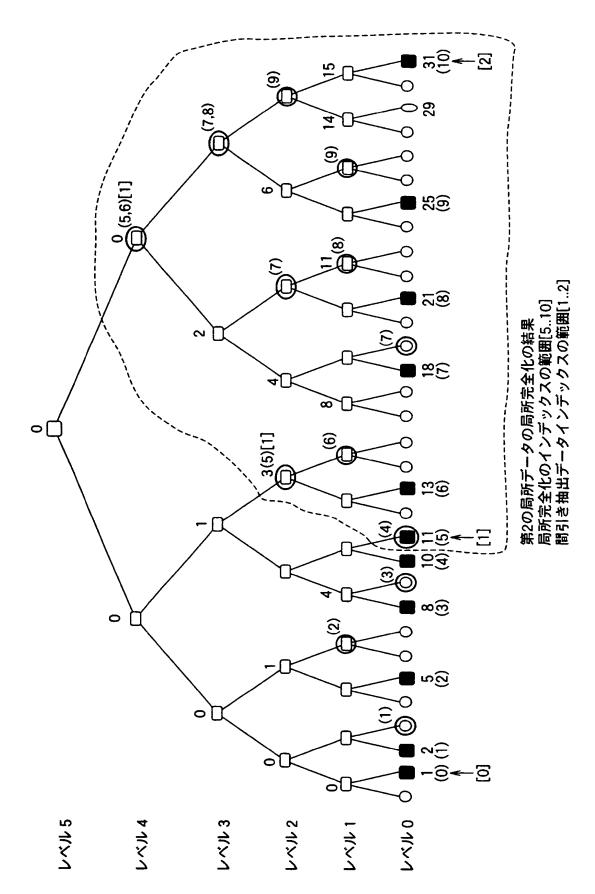


[図72]

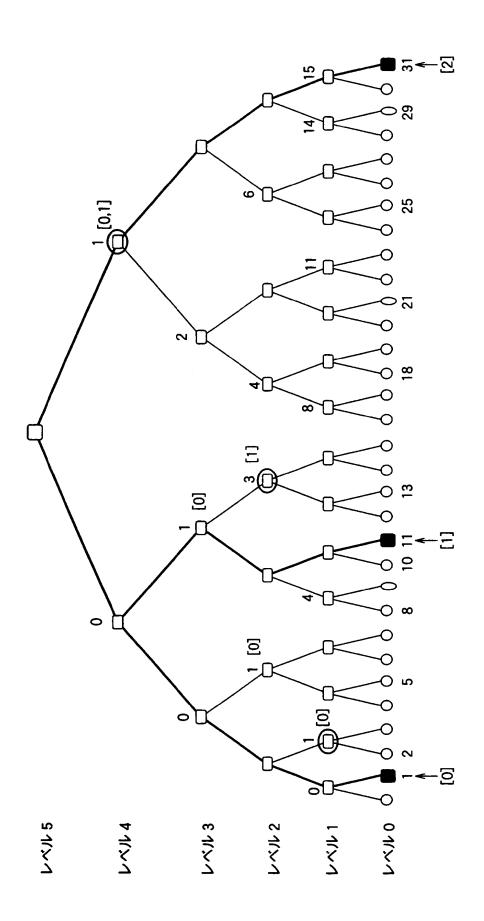


WO 2006/019143 PCT/JP2005/015085 67/77

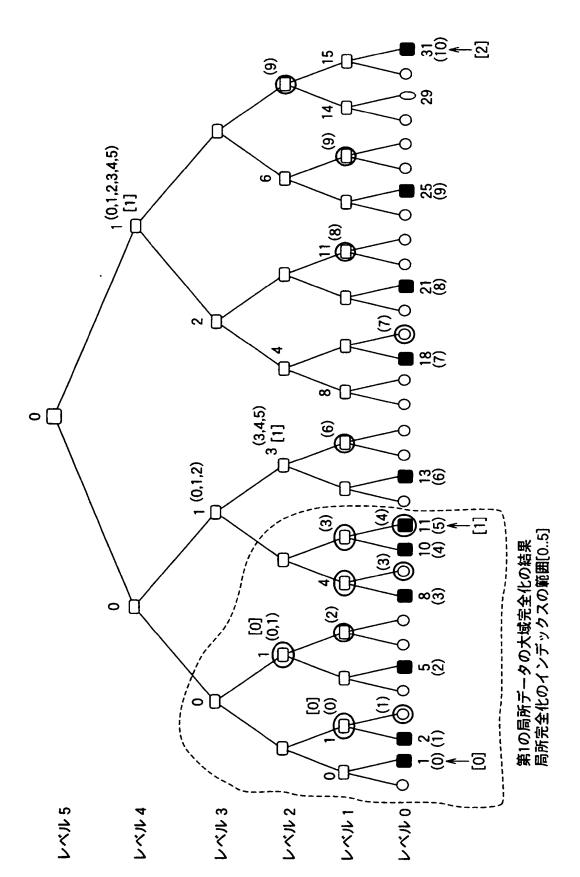
[図73]



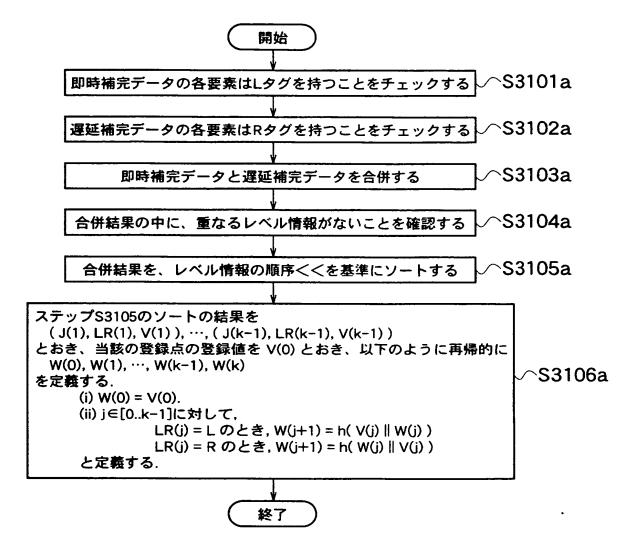
[図74]



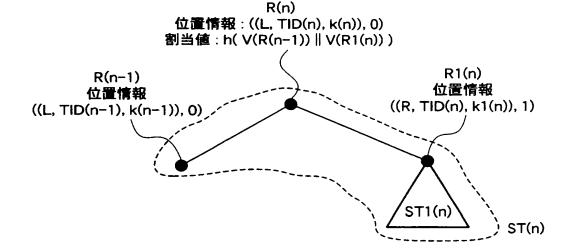
[図75]



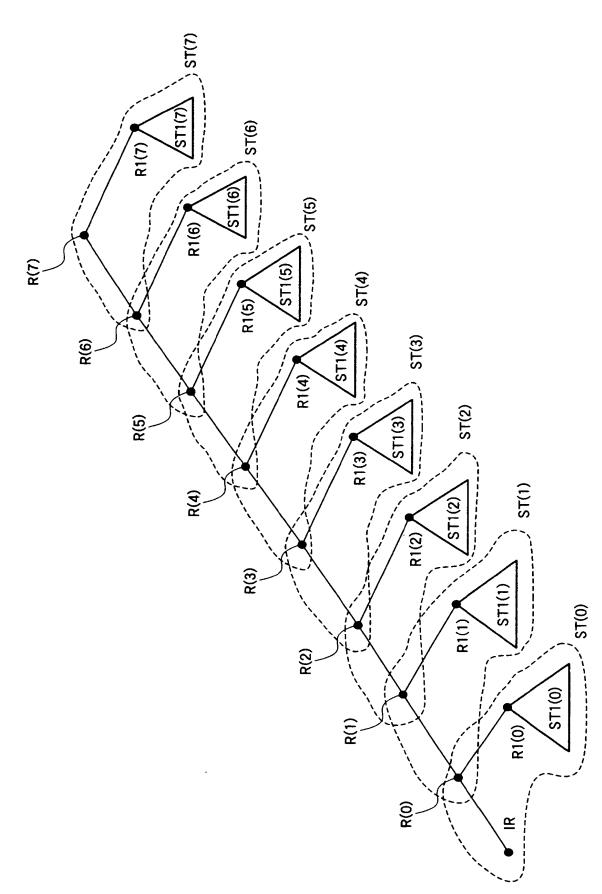
[図76]



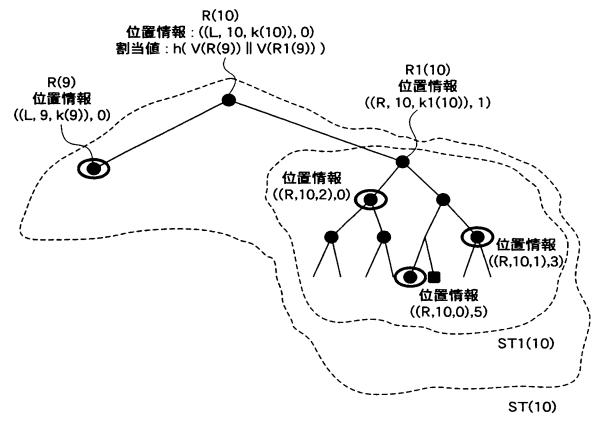
[図77]



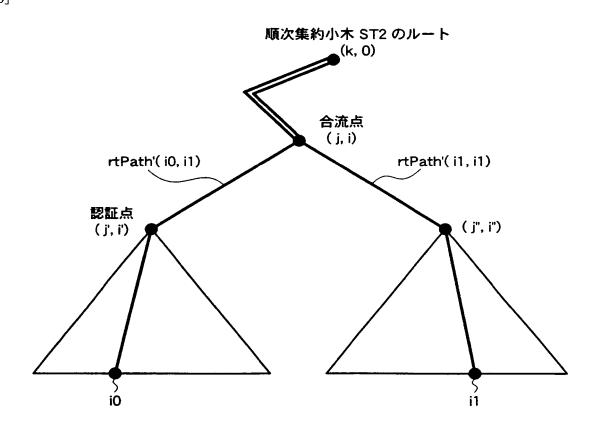
[図78]



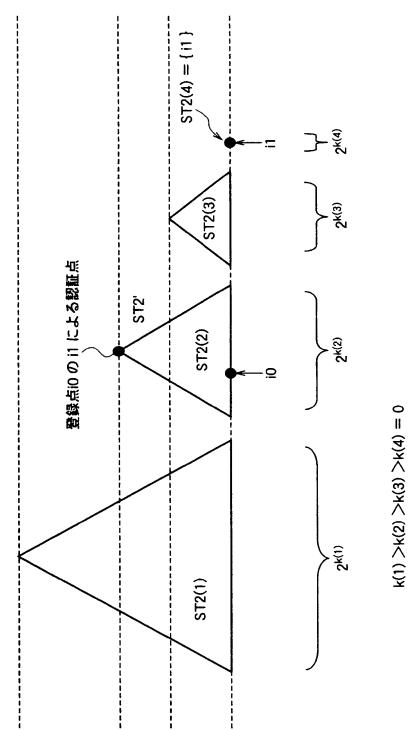
[図79]



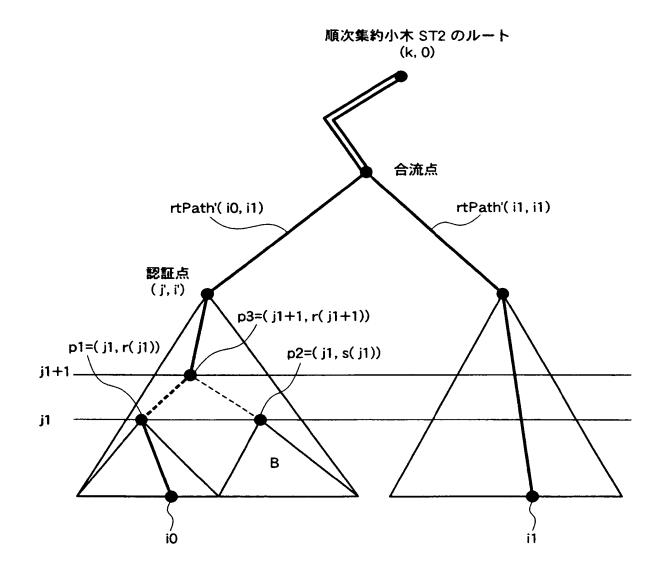
[図80]



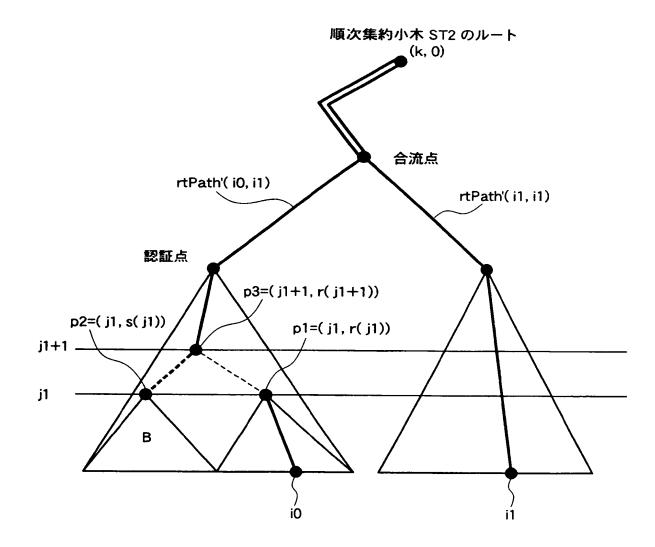
[図81]



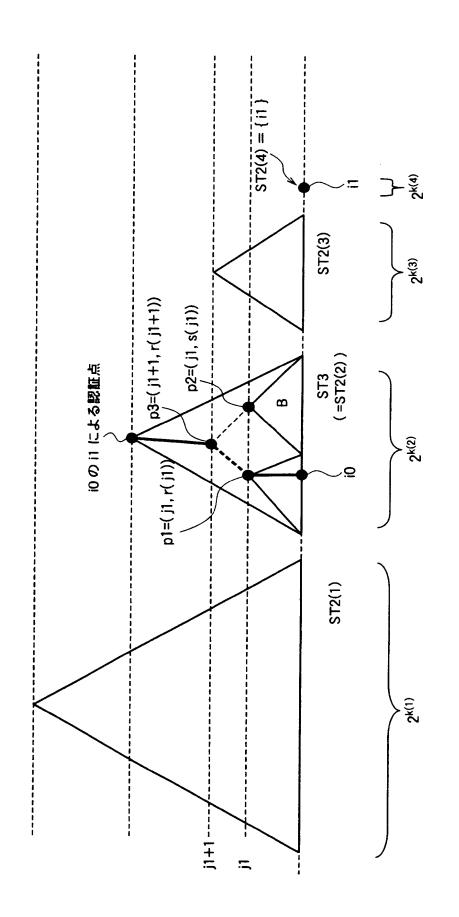
[図82]



[図83]

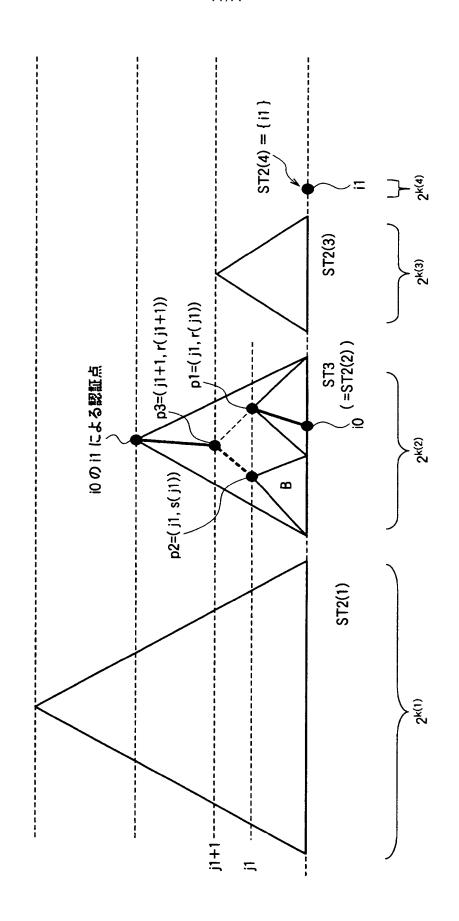


[図84]



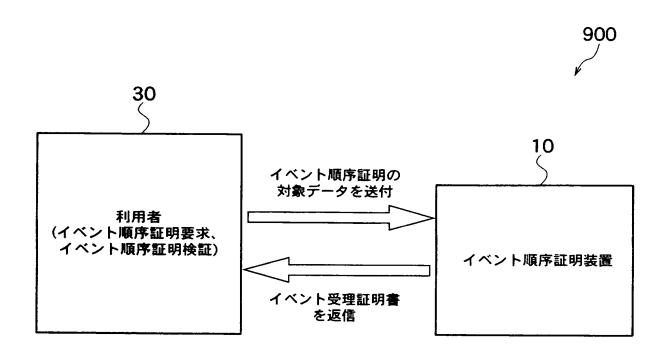
k(1) > k(2) > k(3) > k(4) = 0

[図85]

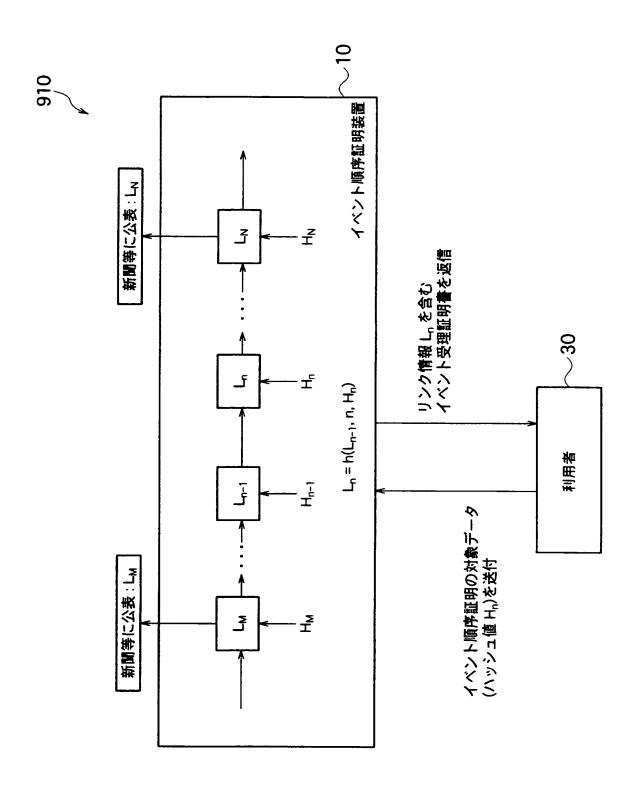


k(1) > k(2) > k(3) > k(4) = 0

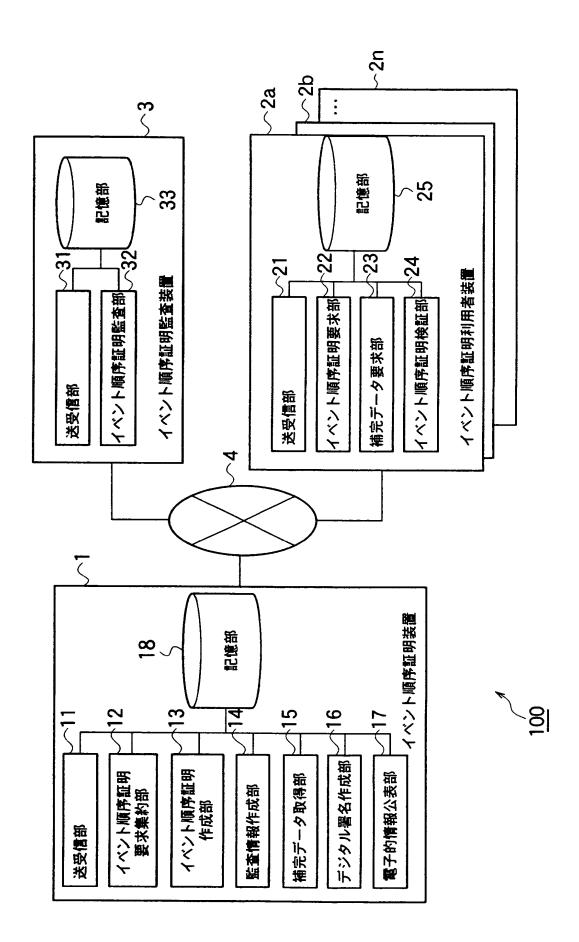
[図1]



[図2]



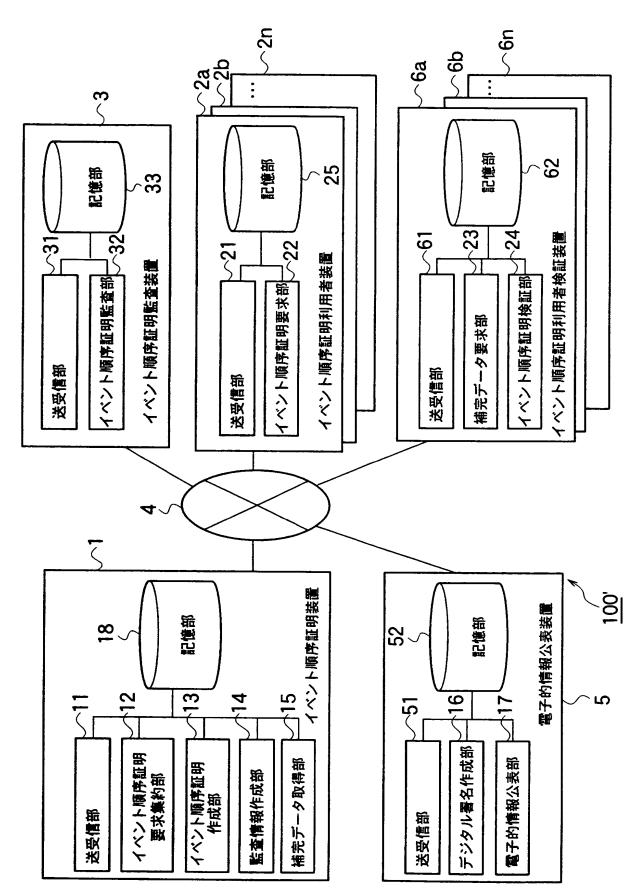
[図3]



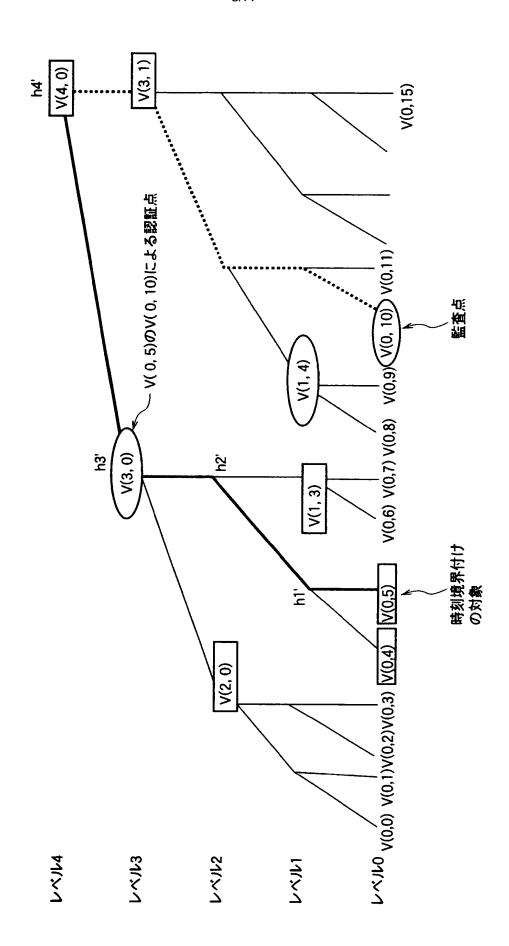
WO 2006/019143 PCT/JP2005/015085

4/77

[図4]



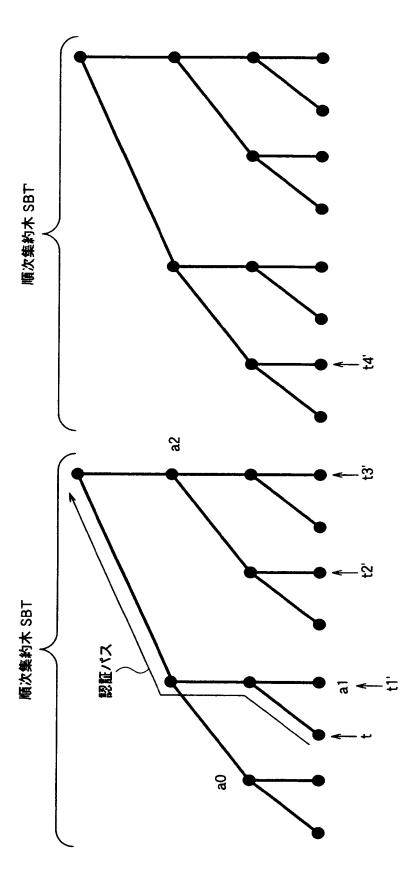
[図5]



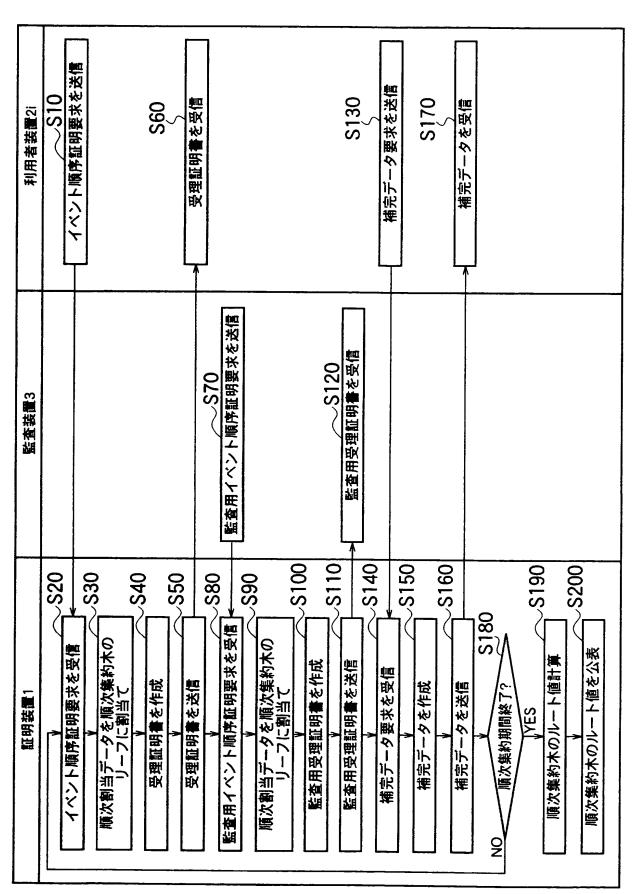
WO 2006/019143 PCT/JP2005/015085 6/77

[図6]

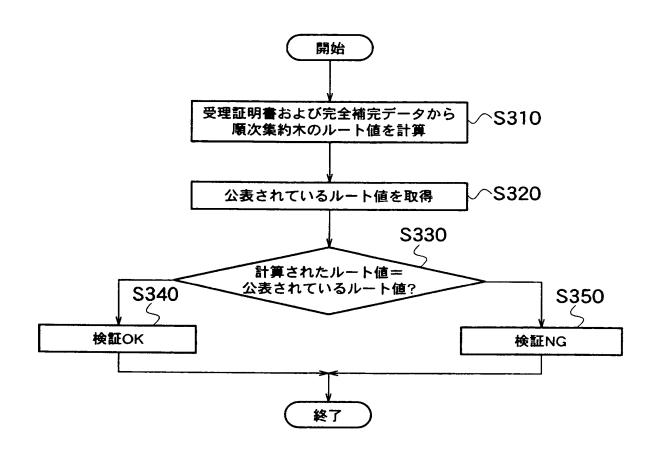
項目	記号	必須
元デジタルデータ	у	0
順次割当データ	z	0
順次集約木番号	n	0
順次集約木リーフ番号	i	0
即時補完データ(位置情報、割当値)	НК	
デジタル署名	DS	



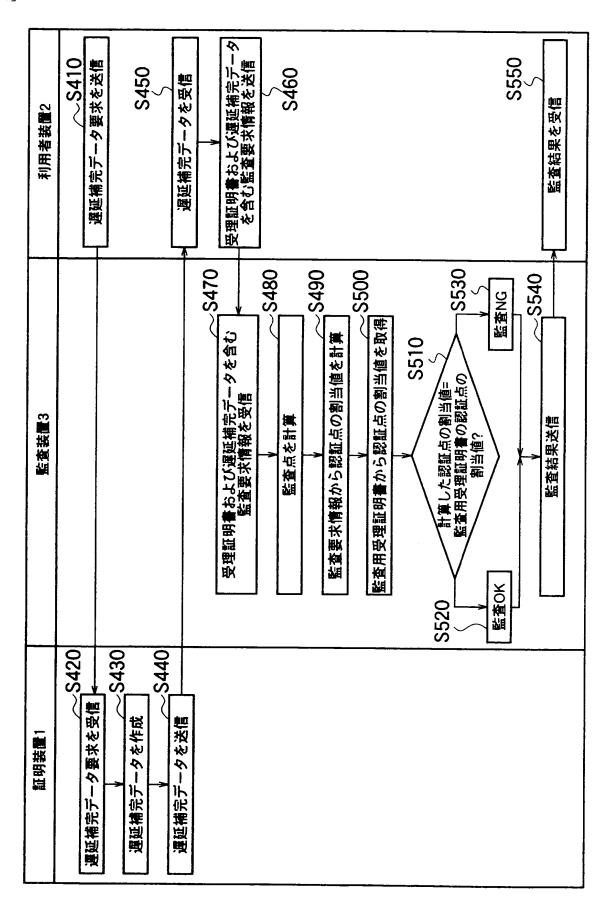
[図8]



[図9]



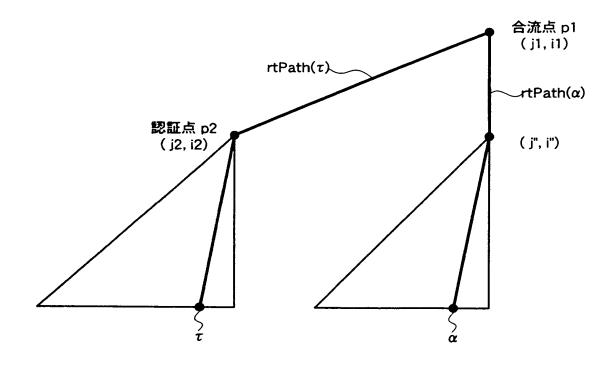
[図10]



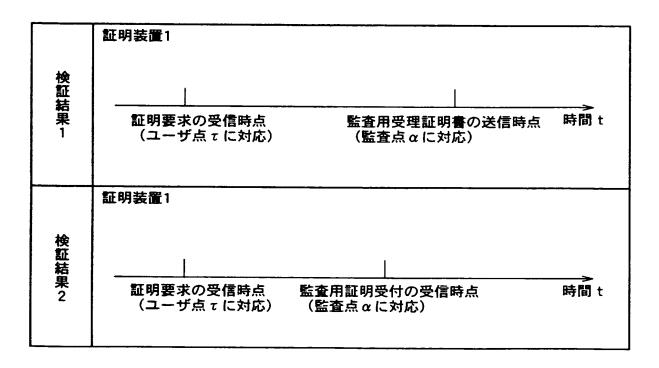
WO 2006/019143 PCT/JP2005/015085

11/77

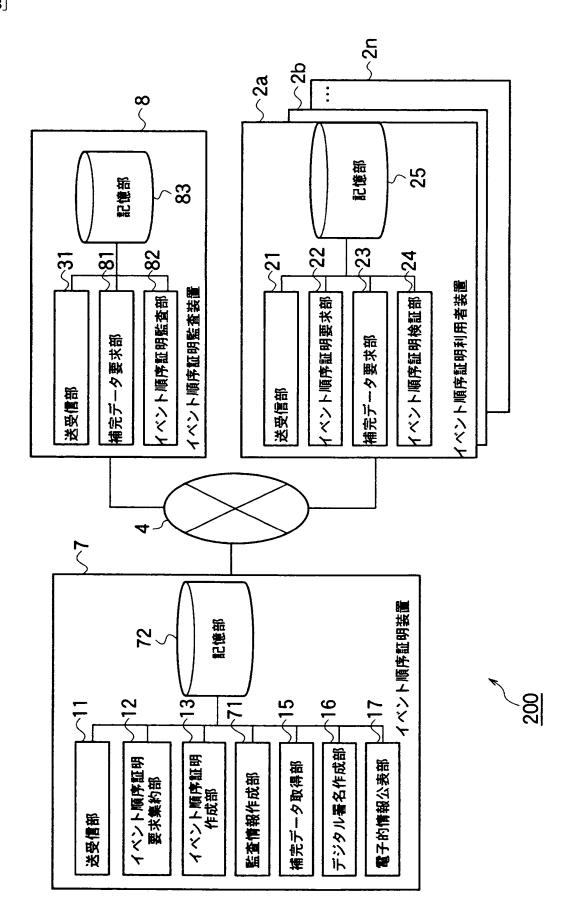
[図11]



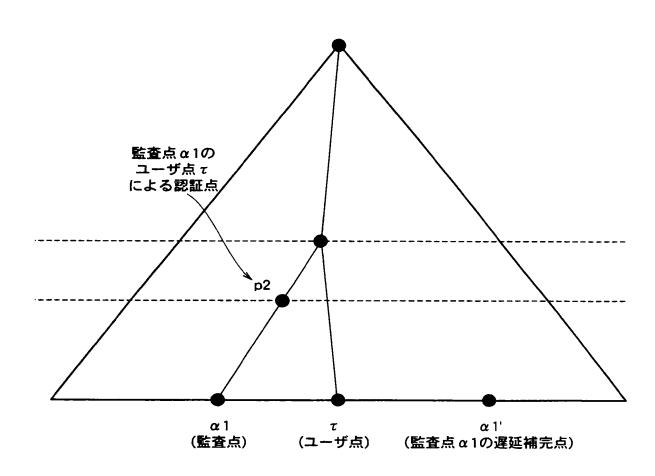
[図12]



[図13]



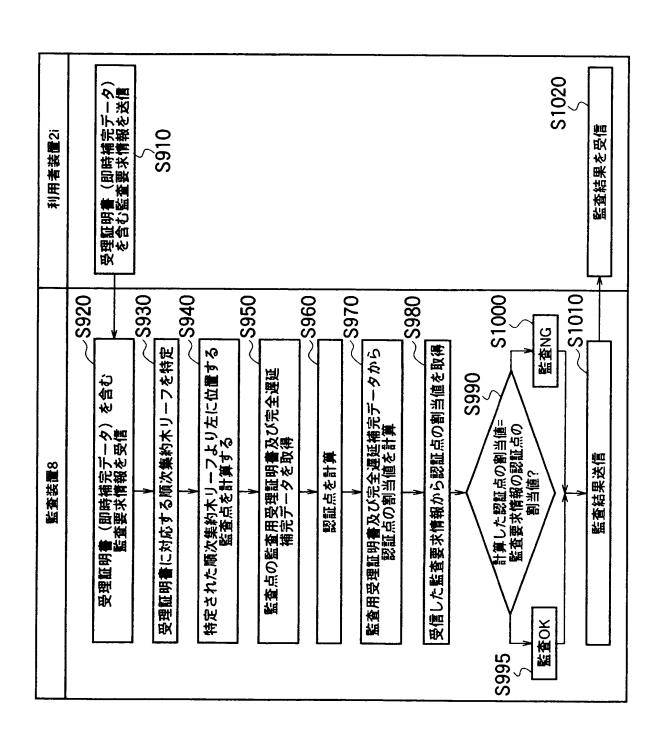
[図14]



[図15]

利用者装置2.	~S610	イベント順序証明要求を送信	099S	受理証明書を受信	\$730 \$	#完データ要求を送信 S770 5 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	開元ナータを受信	
8. 票菜 墓籍				S670 監査用イベント順序証明要求を送信	S720 ★ 監査用受理証明書を受信			S810 完全遅延補完データ要求を送信 S830 監査用受理証明書の 完全遅延補完データを受信
証明装置7			受理証明書を作成 S650	受理証明書を送信 監査用イベント順序証明要求を受信 原次割当データを順次集約木の	リーフに割当て 監査用受理証明書を作成 監査用受理証明書を送信 を表別	\mathbf{v}	NO 順次集約期間終了? S780 TYES S790 S790 TYES S790 S790	順次集約木のルート値を公表

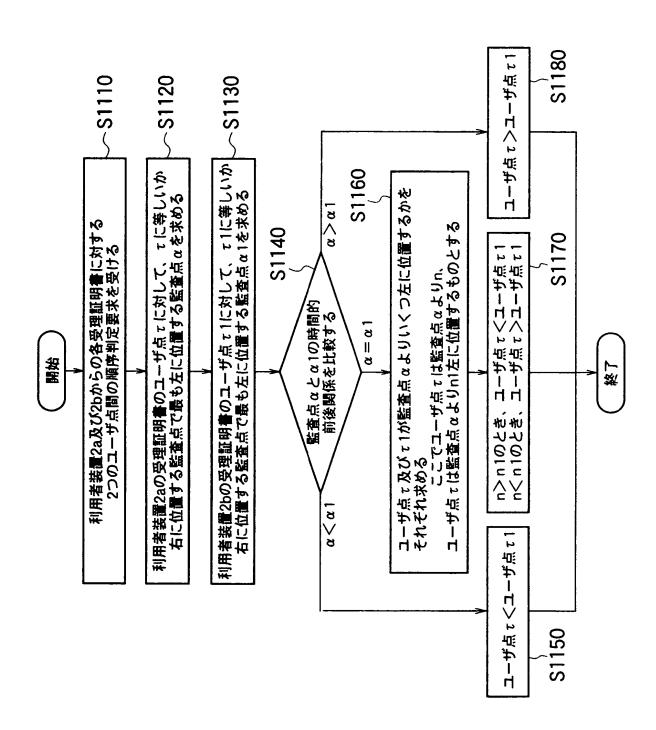
[図16]



WO 2006/019143 PCT/JP2005/015085

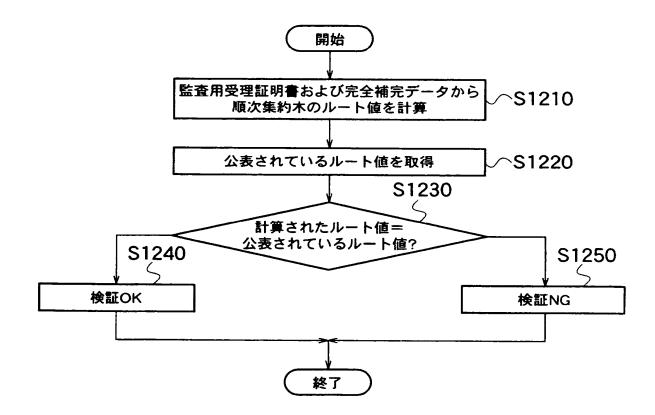
16/77

[図17]



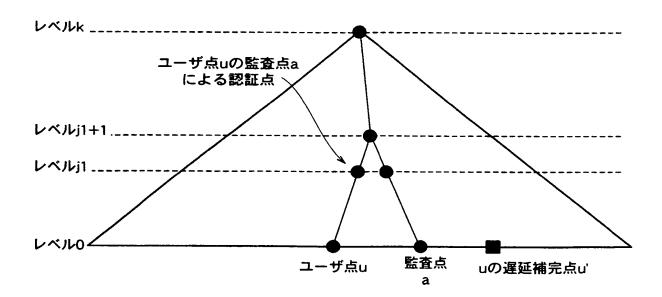
WO 2006/019143 PCT/JP2005/015085 17/77

[図18]

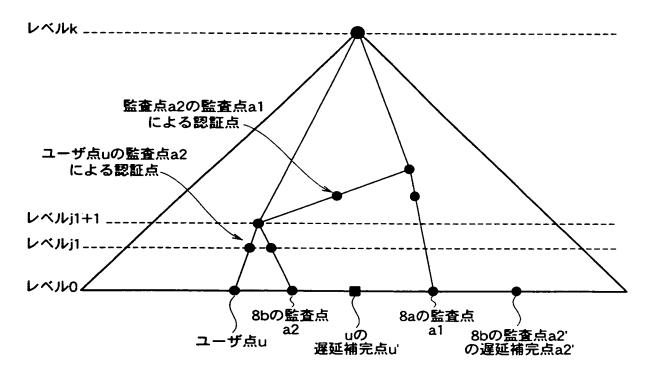


WO 2006/019143 PCT/JP2005/015085

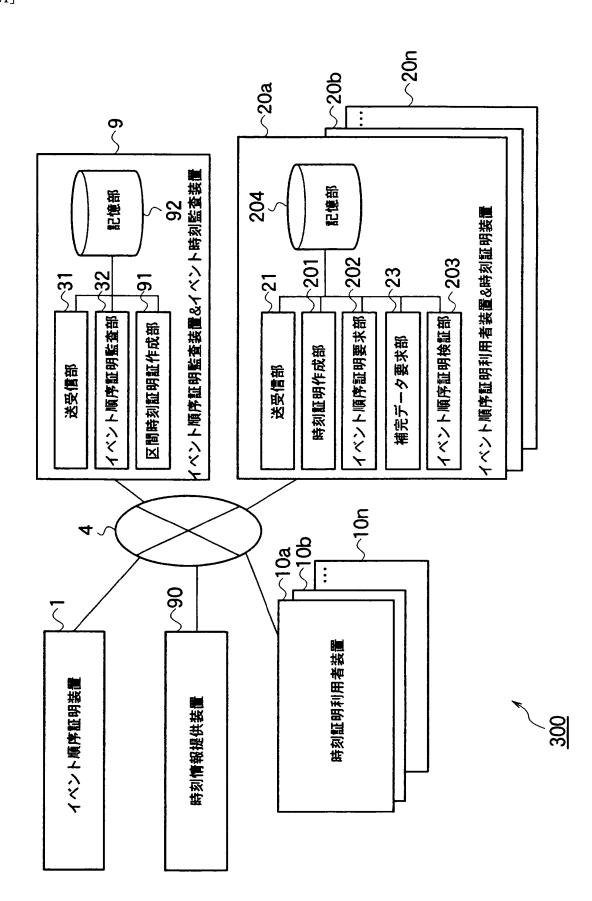
[図19]



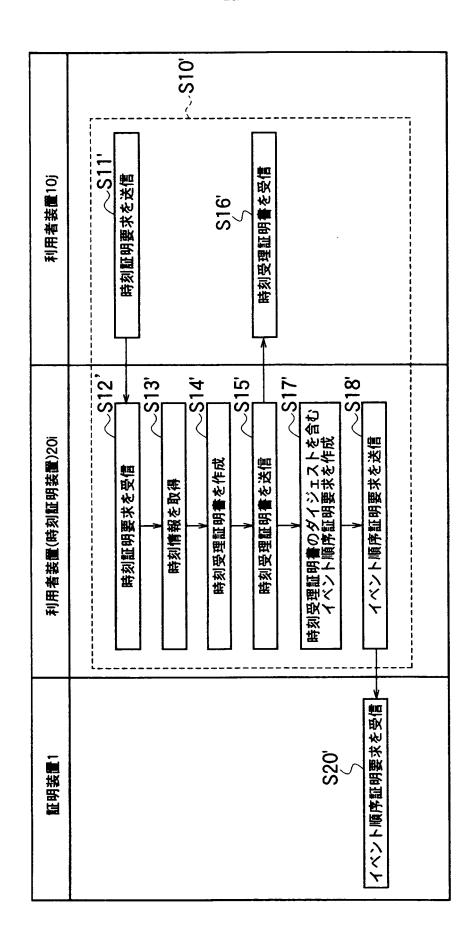
[図20]



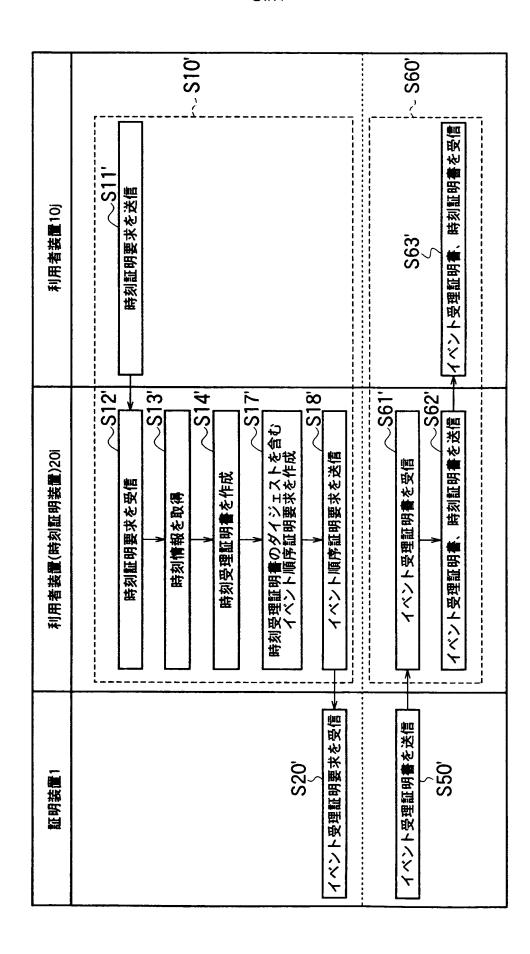
[図21]



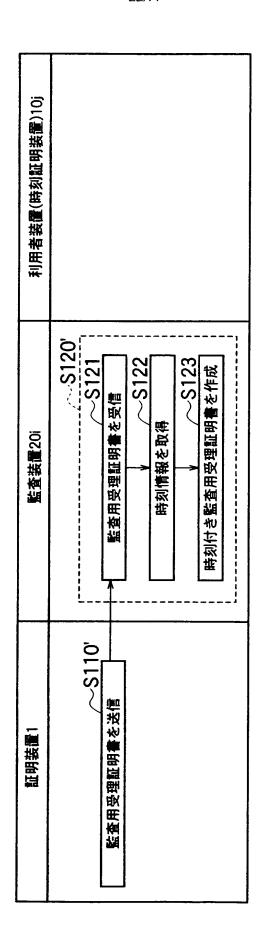
[図22]



[図23]



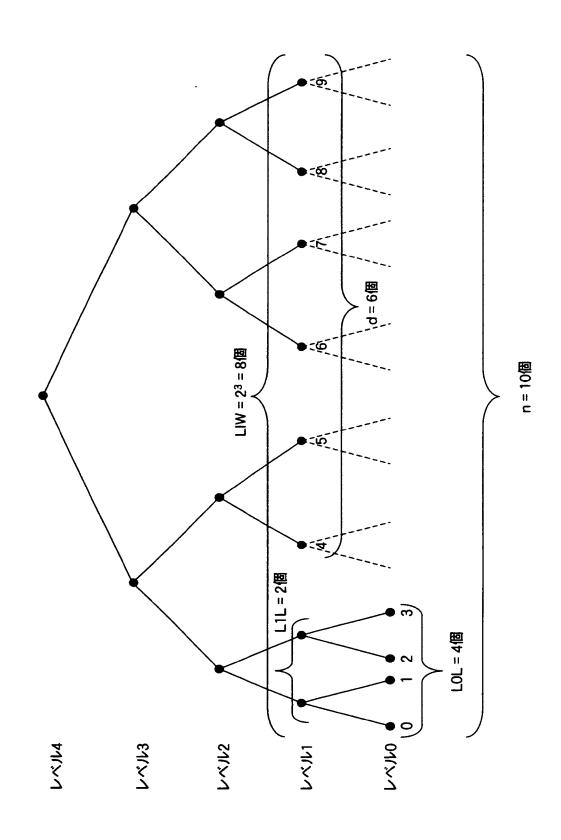
[図24]



[図25]

証明装置1	!02團築垦獨	利用者装置(時刻証明装置)10]
	.01 9 S	
	監査OK	
	√ ~S512'	
	区間時刻証明証を発行	
	√ ~S513'	
	区間時刻証明証を監査結果に含める	

[図26]



[図27]

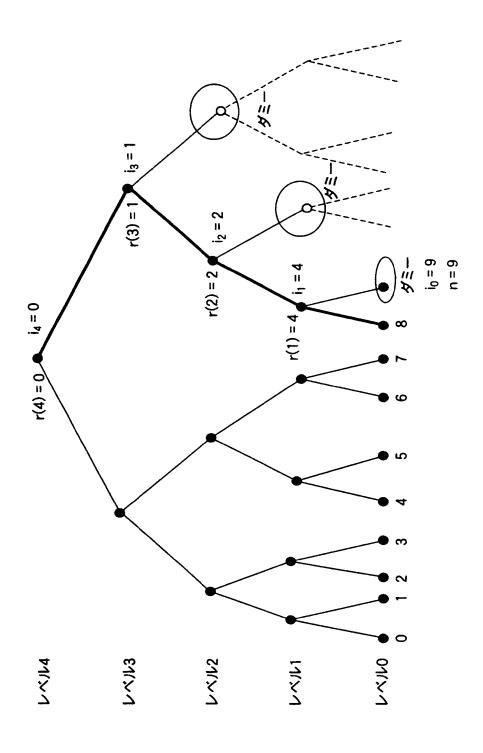
```
(1) ループ1: 構成法その3では、定められた時間間隔が終了するまで
             以下の処理を繰り返す.
   (1.1) 受け付けた要求をxに置く.
   (1.2) nを1インクリメントする.
   (1.3) ループ2: j=0,.., Kに対して以下の処理を行う.
       (1.3.1) i:=ijと置く.
       (1.3.2) j = 0のときは、A<sub>i</sub>[i]:=x
            (即ち、ノード(j, i,)にxを設定する).
       (1.3.3) j > 0のときは、以下を行う。
           x0 : = A<sub>i-1</sub>[index(leftChiild(j, i))]
           (ノード(j,i)のleft-childに割り付けられた値をx0と
            おく).
           * x1 : = A<sub>i-1</sub>[index(rightChild(j, i))]
           (ノード(j,i) のright-childに割り付けられた値をx1と
            おく).
           ・x2:=h(x0 || x1)を計算する.
           • A:[i] : = x2
           (即ち、ノード(j, i) にx2を割り付ける).
       (1.3.5) iが偶数のときは、ループ2を抜ける.
     ループ2終了、
 ループ1終了.
```

処理手順1

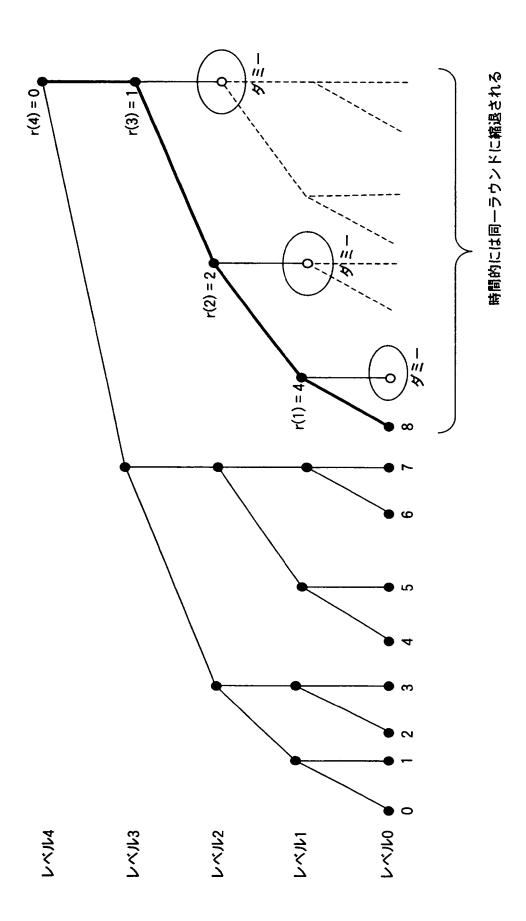
処理手順(

```
(2)終了時間がきて、ループ1を抜けた後では次の処理を行う.
    (2.1) k : = ceiling(log<sub>2</sub>(n))とおく.
    (2.2) rtPath(k,0, n-1) を計算し、その結果を((0, r(0)), ..., (k,r(k)))と置く.
    (2.3) ループ3: j = 0, ..., kに対して以下の処理を行う.
        (2.3.1) i = i<sub>i</sub>とおく.
        (2.3.2) j = 0のとき:
             (2.3.2.1) i が奇数のとき:
                  ・ダミー値 r:= R(0,i) を生成する.
                  • A;[i] : = r
                   (ノード(O, i) にrを割り当て).
                  ・b<sub>i</sub>:= trueと置く.
                  ・i; を1インクリメントする.
        (2.3.2) 0 <j ≤ kのとき:
             (2.3.2.1) i = r(j) のとき:
                     (即ち、ノード(j, i) が rtPath(k, 0, n-1) 上にあるとき):
                  (2.3.2.1.1) \times 0 := A_{i-1}[index(leftChiild(j, i))]
                    (ノード( j, i) のleft-childに割り付けられた値をx0と置く).
                 (2.3.2.1.2) \times 1 := A_{i-1}[index(rightChild(j, i))]
                    (ノード(j, i) Oright-childに割り付けられた値をx1と置く).
                  (2.3.2.1.3) x2 := h(x0 || x1)を計算する
                  (2.3.2.1.4) A[i] := x2
                     (即ち、ノード(j,i) にx2を割り付ける).
                 (2.3.2.1.5) iが偶数で jくk のとき:
・i を1インクリメントする.
・r:=R(j, i)を計算し、Aj[i]:=r
                    (即ち、ノード(j,i) にrを割り当る).
                    ・b<sub>j</sub>:=trueと置く.
                   ・ i<sub>i</sub> := i+1と置く.
             (2.3.2.2) i = r(j)+1で i が奇数で j≪k のとき:
                  ・r:=R(j,i)を計算し、A[i]:=r
                       (即ち、ノード(j,i) にrを割り当る).
                  ・ b<sub>i</sub>:=trueと置く.
                  ・i<sub>i</sub>を1インクリメントする.
      ループ3終了.
```

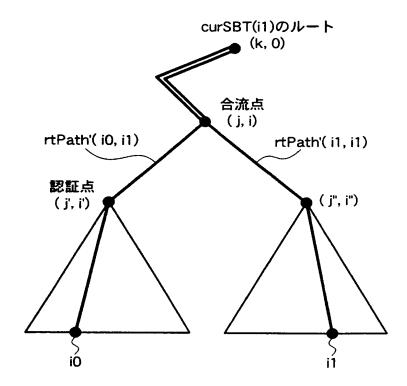
[図29]



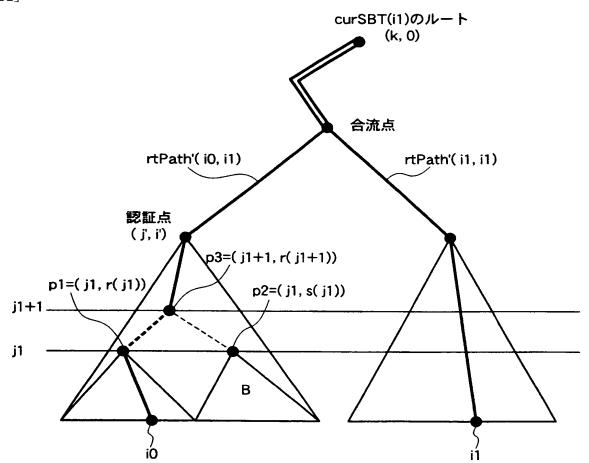
[図30]



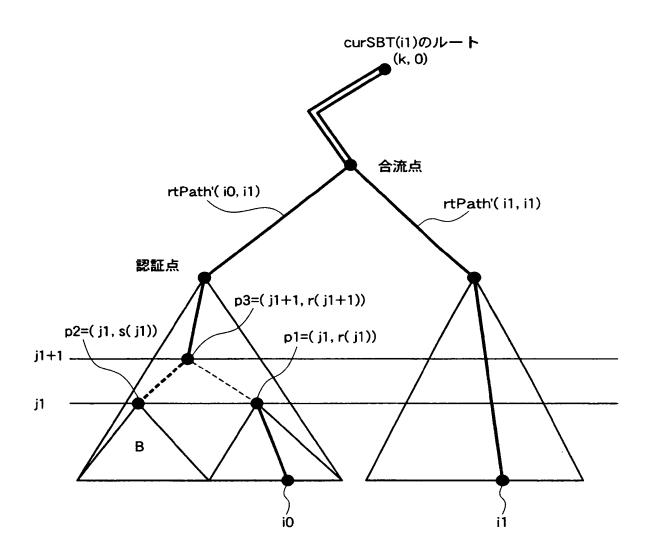
[図31]



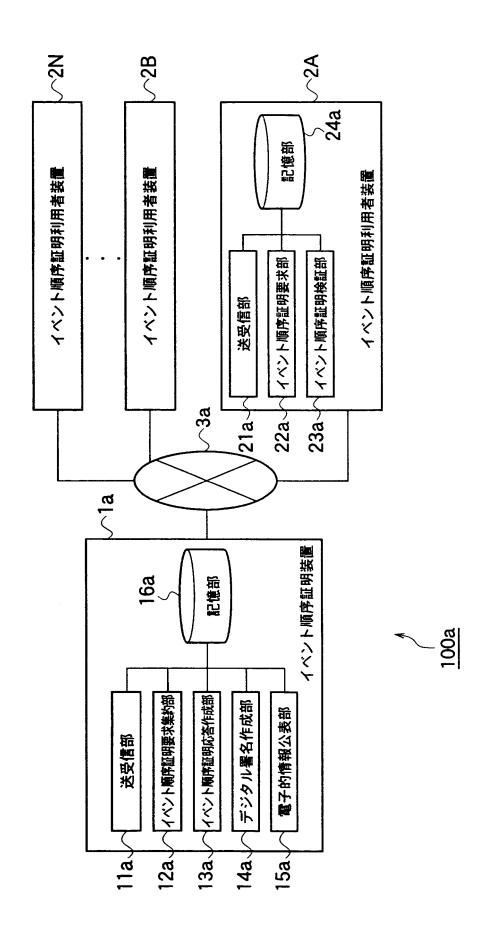
[図32]



[図33]



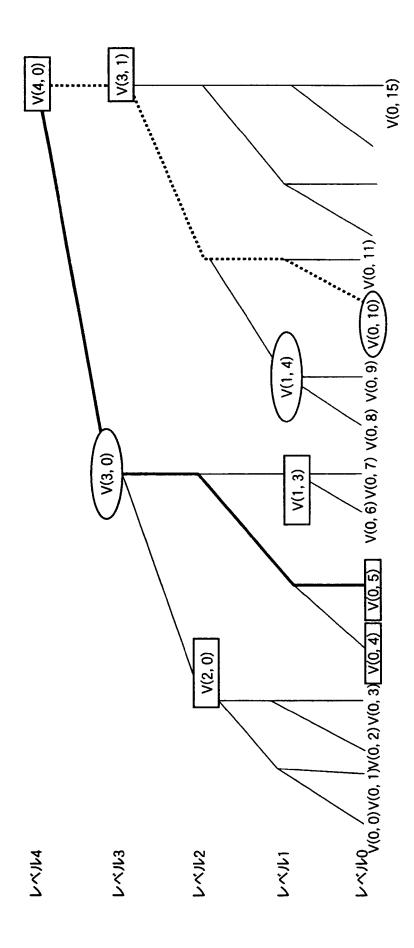
[図34]



32/77

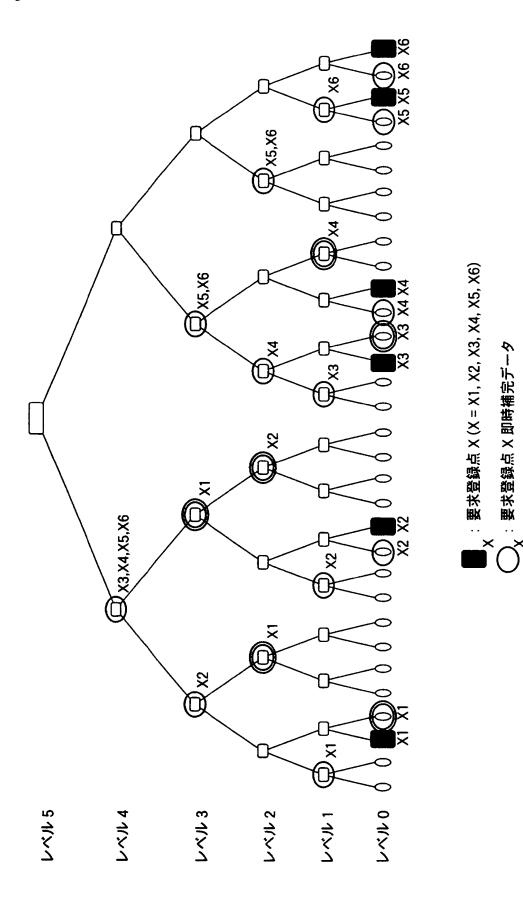
PCT/JP2005/015085

[図35]



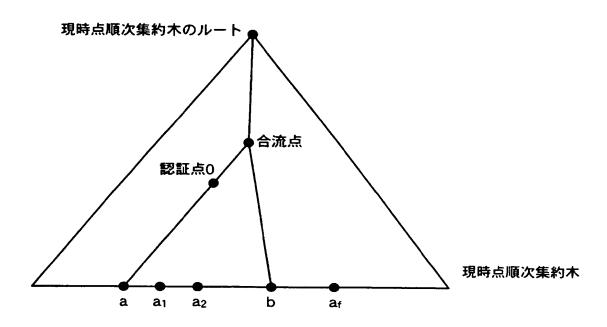
[図36]

	l	ſ	
項目	記号 必須	必須	
元デジタルデータ	>	0	
順次割当データ	2	0	
順次集約木番号		0	人 イベント順序受理証明4 FOC(2)
順次集約木リーフ番号		0	9
登録点の即時補完データ(位置情報、割当値)	×	0	
過去の各登録点の遅延補完データ(位置情報、割当値)	¥	0	



: 要求登録点 X 遅延補完データ

[図38]



[図39]

